

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.
A PROFESSIONAL CORPORATION
1776 BROADWAY, SUITE 2000
NEW YORK, N.Y. 10019

GERALD B. LEFCOURT
lefcourt@lefcourtlaw.com

TELEPHONE
(212) 737-0400
FACSIMILE
(212) 988-6192

—
SHERYL E. REICH
reich@lefcourtlaw.com
FAITH A. FRIEDMAN
ffriedman@lefcourtlaw.com

December 12, 2019

VIA ECF

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
United States Courthouse
40 Foley Square
New York, NY 10007

United States v. Kukushkin, et al. 19 CR. 725 (JPO)

Dear Judge Oetken:

We are counsel to Andrey Kukushkin, a defendant in the above referenced matter. We write on behalf of all defendants with regard to the defense's request pursuant to 18 U.S.C. § 3504, that the government be required to (a) inquire of government agencies and "affirm or deny" whether the defendants' oral or wire communications, including written communications, have been intercepted by means other than Title III or FISA warrants,¹ including by means of Executive Order 12333 ("E.O. 12333") and other surveillance; and (b) if so, to identify such evidence and delineate all fruits thereof.

The Government's Covert Surveillance of United States Citizens

The Foreign Intelligence Surveillance Act ("FISA") was enacted in 1978. It was the result of extensive multi-year investigations into unlawful executive branch domestic surveillance activities. Those investigations were prompted by President Richard Nixon's use of federal resources, including law enforcement, to spy on political and activist groups. FISA was created to provide oversight, both judicial and congressional, of the government's covert

¹ The government has denied procuring evidence pursuant to Title III or FISA warrants.

LAW OFFICES OF

GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 2

surveillance activities within the United States related to matters of national security, and is meant to proscribe surveillance of United States persons pursuant to the Act in all but limited circumstances.

In 1981, President Ronald Reagan signed E.O. 12333. It is the primary authority for the NSA's foreign intelligence gathering. Addressed to "detecting and countering" "[t]hreats to the [United States] and its interests from terrorism" it authorizes intelligence agencies to create policies and procedures to accomplish E.O. 12333's goals without court involvement or oversight. The breadth of E.O. 12333 is so far reaching that even though directed to activities outside the United States by foreign persons and governments, it permits the collection, retention, and dissemination of information concerning United States persons that is "incidentally obtained", if that information "may indicate involvement in activities that may have violated Federal, state, local, or foreign law". E.O. 12333, Part 2, § 2.3(i). With this broad directive, the advent of more advanced surveillance techniques, and global interconnectedness, it is not surprising that the line between domestic and foreign surveillance has blurred, and along with it the line between FISA surveillance (requiring notice and judicial process) and E.O. 12333 surveillance (which the government contends can be maintained in secrecy and insulated from judicial review).

We now know United States agencies have the ability to and under the auspices of E.O. 12333 engage in bulk surveillance programs, not subject to judicial or congressional oversight,² by which they (1) collect metadata and audio files of every cell phone call to, from and within certain countries;³ (2) intercept the private data of hundreds of millions of Google and Yahoo

² Per the NSA, "FISA only regulates a subset of NSA's signals intelligence activities. NSA conducts the vast majority of its SIGINT [signal intelligence] activities solely pursuant to the authority provided by Executive Order (EO) 12333". NSA Legal Fact Sheet: Executive Order 12333 (June 19, 2013).

³ Amos Toh, Faiza Patel, & Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, Brennan Center, March 16, 2016, at p. 5

(www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf) ("Under a program codenamed NYSTIC, the NSA fathers information about every cell phone call made to, from and within the Bahamas, Mexico, Kenya, the Phillipines, and Afghanistan... In the Bahamas and Afghanistan, the NSA ... goes further and stores for thirty days an audio recording of every cell phone call placed to, from, and within these countries using a system codenamed SOMALGET... the NSA reportedly intends to expand the program to more countries and may already have done so"); see also Patrick C. Toomey et al., ACLU Letter to Privacy and Civil Liberties Oversight Board, January 13, 2016, at pp. 5-7 (www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333).

LAW OFFICES OF

GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
 United States District Judge
 Southern District of New York
 December 12, 2019
 Page 3

customers as it is routed to data centers outside the United States;⁴ (3) conduct “backdoor searches” of Section 702 data for information about U.S. persons;⁵ (4) collect personal information from email and instant messaging accounts, many belonging to Americans;⁶ and (5) conduct daily sweeps of text messages around the world.⁷ And if that were not enough, law enforcement efforts to avoid disclosure of such techniques, including through a process aptly entitled “parallel construction”, also are well documented. See Sarah St. Vincent, *Dispatches: U.S. Surveillance Court Opinion Shows Harm to Rights*, Human Rights Watch, April 22, 2016 (detailing government “use” of data seized under § 702 FISA in the investigations of “any federal crime” but noting apparent policy of non-disclosure to criminal defendants”); see also B. Heath, *FBI Warned Agents Not To Share Tech Secrets With Prosecutors*, USA Today, April 20,

⁴ Charlie Savage, *Reagan-Errol Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, August 13, 2014 (“Large email companies like Google and Yahoo have built data centers abroad, where they store backups of their users’ data. Mr. Snowden disclosed that in 2012 the N.S.A....penetrated links connecting the companies’ overseas data centers and collected 181.3 million records in 30 days”).

⁵ Ronald Newman and Neema Singh Guiliani, *ACLU Letter to U.S. Senate Judiciary Committee*, November 5, 2019, (www.aclu.org/letter/aclu-statement-record-senate-judiciary-committees-reauthorizing-usa-freedom-act-2015-hearing) (“Section 702 explicitly prohibits the government from targeting U.S. persons. The government nevertheless searches Section 702 data looking specifically for information about U.S. persons, a practice often referred to as a “backdoor search.” This permits Section 702 to be exploited as a tool against Americans in foreign intelligence and domestic criminal investigations alike....While the FBI refuses to report the number of backdoor searches it performs, the Privacy and Civil Liberties Oversight Board reports that the number of these searches is ‘substantial,’ in part because it is ‘routine practice’ for the FBI to conduct a query when an agent initiates a criminal assessment or investigation related to any type of crime”) citing Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Sec. 702 of the Foreign Intelligence Surveillance Act*, July 2 2014 (<https://www.pclob.gov/library/702-Report.pdf>).

⁶ Barton Gellman & Ashkan Soltani, *NSA Collects Millions of Email Address Books Globally*, Washington Post, October 14, 2013 (https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html) (“During a single day last year, the NSA’s Special Source Operations branch collected 444,743 e-mail address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers, according to an internal NSA Powerpoint presentation. Those figures, described as a typical daily intake in the document, correspond to a rate of more than 250 million a year.... Although the collections take place overseas, two senior U.S. intelligence officials acknowledged that it sweeps in the contacts of many Americans... likely to be in the millions or tens of millions”).

⁷ Amos Toh, Faiza Patel, & Elizabeth Goitein, *supra*, at p. 6, (“The NSA uses a program codenamed DISHFIRE to gather the content and metadata of hundreds of million of text messages from around the globe, and stores the information in a database that is also accessible to [British intelligence]”).

LAW OFFICES OF

GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 4

2016 (“...there’s usually no need for the case agents or prosecutors to know how something was done”.); Savage, *supra* at note 4 (government avoids using E.O. 12333 information as direct evidence in criminal cases “so as not to have to divulge its origins ... in court...officials contend that defendants have no right to know if 12333 intercepts provided a tip from which investigators derived other evidence”.); Brian Fung, *The NSA Is Giving Your Phone Records to the DEA and the DEA is Covering It Up*, Washington Post, August 5, 2013; Shiffman & Cooke, *Exclusive: U.S. Directs Agents To Cover Up Program Used To Investigate Americans*, Reuters, August 5, 2013 (“federal agents are trained to ‘recreate’ the investigative trail to effectively cover up where the information originated...”).

Procedural Background

With this backdrop, in the days leading up to and following his arraignment, Mr. Kukushkin’s counsel sought to discover whether in the course of its investigation Mr. Kukushkin’s communications were intercepted or overheard by the government. After all, among other things, the charges involved foreign nationals, foreign money, and foreign communications, and the indictment contained what the government purports are direct quotes of messages between the defendants. The government responded by advising counsel that no Title III warrants or intercepts had been obtained as part of the investigation. The defense specifically inquired as to whether non-Title III interceptions had been authorized or obtained, including as a result of FISA warrants, National Security Letters, or any other form of NSA or intelligence agency surveillance, which would include all Executive Order (“E.O.”) 12333 surveillance. Curiously, the government’s response remained that “the government did not obtain or use Title III intercepts” during its investigation.

Not satisfied with the government’s oral representations, on November 26, 2019, Mr. Kukushkin submitted a written request pursuant to 18 U.S.C. §3504, that the government conduct a search of the appropriate agencies and “affirm or deny” whether Mr. Kukushkin’s communications were intercepted by means other than a Title III warrant. *See* Exhibit “A”. On December 1, 2019, the government again responded that it did not obtain or use Title III intercepts during the course of this investigation. *See* Exhibit “B”. In addition, the government, without denying its existence, stated that it “does not intend to use any information that was obtained or derived from the Foreign Intelligence Surveillance Act or the other forms of surveillance identified” in Mr. Kukushkin’s request. *Id.* The government further contended that the defense had not presented a sufficient basis for its request and that the request was premature

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 5

because it applies only to “proceedings and not discovery”. *Id.* The government reiterated the same arguments when the issue was raised during the December 2, 2019 status conference.

The government has no basis to refuse the defendants’ request and should be ordered to conduct an inquiry of its agencies and “affirm or deny” whether the defendants’ oral or written communications were subject to surveillance and/or intercepted by the government by means other than a Title III warrant, and whether any evidence the government presented to the grand jury or which it intends to introduce at trial was obtained in this manner or otherwise derived therefrom.

Applicable Law

Oral and written communications intercepted in violation of federal law and the United States Constitution are not admissible. The prohibition applies equally with respect to evidence sought to be admitted at trial and that sought to be admitted in any grand jury proceeding. 18 U.S.C. § 2515. The fruits that flow from that evidence are similarly inadmissible. *Id.*; *Gelbard v. United States*, 408 U.S. 41, 46 (1972); *Wong Sun v. United States*, 371 U.S. 471, 486-88 (1963) (explaining “fruit of the poisonous tree” doctrine); *Murray v. United States*, 487 U.S. 533, 536-37 (1988) (as to right to seek suppression of evidence “derived” from an unlawful search).

In order to vindicate and protect their rights, defendants are entitled to test – in an adversarial proceeding – whether the government’s evidence is the direct product of or derived from illegal surveillance. *United States v. U.S. District Court*, 407 U.S. 297 (1972) (unanimously declaring non-court ordered interceptions illegal and violative of the Fourth Amendment) (“Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President’s domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment”).; *Alderman v. United States*, 394 U.S. 165 (1969); *see also*, *Wong Sun v. United States*, 371 U.S. at 486-88 (1963); *Murray v. United States*, 487 U.S. at 536-37. Of course, before one can seek to suppress illegally obtained evidence and the fruits thereof, the existence of such evidence and the manner by which it was obtained must be ascertained. Put another way, without notice of the evidence and discovery with respect to the means by which it was collected, a court has no mechanism to “provide the

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 6

scrutiny which the Fourth Amendment exclusionary rule demands”. *Alderman v. United States*, 394 U.S. at 184, 184-85; *see also, Berger v. New York*, 388 U.S. 41, 60 (1967).

Section 3504 was enacted to benefit and protect the rights of victims of illegal electronic surveillance. *See Hearings on S. 30 Before Subcomm. No. 5 of the House Comm. On the Judiciary*, 91st Cong., 2nd Sess. 84, 104 (1970); *see also Gelbard v. United States*, 408 U.S. at 56. The statute provides that “upon a claim” by a defendant that either direct or derivative evidence was the subject of an unlawful seizure, the government must “confirm or deny” the existence of that purported unlawful seizure:

(a) In any trial, hearing, or other proceeding in or before any court . . . of the United States—

(1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim *shall affirm or deny the occurrence of the alleged unlawful act*.

18 U.S.C. § 3504 (emphasis added). “Unlawful act” is defined as “the use of any electronic, mechanical, or other device . . . in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto”. 18 U.S.C. § 3504(b).

A request pursuant to § 3504, while requiring more than “mere suspicion”, need not be based on a “particularized” claim. All that is necessary is a “colorable basis” to trigger the government’s obligation to inquire and respond. *See United States v. Pacella*, 622 F.2d 640, 643 (2d Cir. 1980); *accord* CRM at 36 (“‘mere assertion’ . . . generally been sufficient to raise a claim under 18 U.S.C. 3504 (*see In re Evans*, 452 F.2d 1239, 1247 (D.C. Cir. 1971), *cert. denied*, 408 U.S. 930)”, although “there is some indication that courts are beginning to raise the threshold.” *citing e.g. In re Millow*, 529 F.2d 770, 774-775 (2d Cir. 1976) (claim lacks any colorable basis; objection should be raised to the search on that ground)). Once the defendants have met the initial threshold, it is incumbent upon the government to respond.

Of course, in order to comply with its obligations under § 3504, the government must necessarily apprise itself of the facts upon which its response will be based. Accordingly, the Department of Justice has created a procedure, known as the “all agency search”, conducted in

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 7

Washington, D.C. by trained researchers who search records maintained by the government for the purpose of keeping track of electronic surveillance:

Generally, the government has an obligation pursuant to the provisions of 18 U.S.C. § 3504, to conduct a search of the appropriate agencies and to affirm or deny a claim that a defendant has been illegally overheard. This search is initiated at the request of the United States Attorney, to the Policy and Statutory Enforcement Unit of the Office of Enforcement Operations of the Criminal Division, and the results of the check are reported to that office.

Criminal Resource Manual at 36.

The government's conclusory assertions aside, the defendants undoubtedly have established a "colorable basis" sufficient to trigger the government's inquiry obligations, and the government should be ordered to undertake a comprehensive "all agency search". Indeed, if ever a case cried out for the government to conduct such a review and return its findings, this is it.

Colorable Basis For the Request

As congress and the courts recognize, the very nature of the information sought makes it difficult to articulate with any particularity the bases for defendants' request. Defendants who are in possession of compelling "proof" that the government engaged in illegal electronic surveillance need not avail themselves of § 3504, as the acknowledgment of government wrongdoing is unnecessary to proceed with a motion to suppress. Instead, § 3504 is meant to be invoked by those defendants who, although they have a "colorable basis" for their claim, lack the proof necessary to demonstrate their communications were illegally. Such is the case here.

This case involves foreign nationals, foreign government officials, foreign communications, foreign travel, foreign wires, and issues of national security. More specifically, the indictment and search warrant refer to the involvement of a purportedly Russian national (Foreign National-1), residing abroad, who, according to the government, has no legal status in the United States. Allegations of foreign sources of money, including from Russia and South Korea, being used for contributions to Republican linked political committees, including those connected to the President, as well as campaigns of other high-ranking politicians and political candidates, in contravention of federal election laws, also abound. And, the government contends that certain of the defendants in this case undertook efforts to "remove" the former United States

LAW OFFICES OF

GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 8

Ambassador to the Ukraine, “at least in part, at the request of one or more Ukrainian government officials” (indictment at p. 8, ¶17), and that in connection with those efforts those defendants communicated with high-ranking officials of the United States government and worked with Ukrainian government officials.

If that were not enough, many of subjects of the government’s investigation, including some number of the defendants, are alleged and known by the government to have traveled overseas, including within Russia and the Ukraine, during the course of the charged criminal conduct. Indeed, the government cited the defendants’ purportedly vast foreign travel and international connections, including Mr. Parnas’ relationship with an indicted Ukrainian oligarch being sought by the United States for extradition from Vienna, as bases to impose onerous bail conditions and deny any modifications thereto.

In addition, from the recent congressional impeachment inquiry and subsequent congressional reports (in which Mr. Parnas is identified by name), not to mention media reports, it is clear that the allegations involve matters of national security and conduct and communications of United States and foreign political leaders. And from these same sources we know with little doubt that United States intelligence officers and agencies have and continue to be involved in the matter.

Moreover, the government’s own statements demonstrate that there is a “colorable basis” to believe unauthorized surveillance occurred. In the face of repeated and direct requests as to the existence of such evidence, that is interceptions of oral and written communications by means other than Title III warrants, the government has offered not a single denial. Rather, it has engaged in obvious subterfuge, insisting repeatedly the mantra “no Title III warrants were used in this investigation”. Of course, whether Title III warrants were used is not the information the defendants have sought from the government and the government’s insistence on ignoring this fact is telling.

The government fails not better with its averment that “it does not intend to use” such evidence – without acknowledging whether such evidence exists. It too simply begs the question and does not obviate the need for the requested information. The defendants are entitled to know whether the government overheard or intercepted their communication and whether other evidence, particularly evidence that was submitted to the grand jury or which the government intends to introduce at trial, was derived therefrom. *See United States v. Belfield*, 692 F.2d 141, 146 (D.C. Cir. 1982) (in FISA context “even when the Government has purported not to be

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 9

offering any evidence obtained or derive from electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the logs of the overhears to ensure that no fruits thereof are being used against him”).

Nor is the defendants’ request premature. Without authority or further explanation, the government contends that demands under § 3504 are appropriate only to “proceedings not discovery”. The government seemingly ignores that there is a proceeding – this criminal prosecution that will lead to a trial. The argument also ignores, or at least misapprehends, the government’s Rule 16 discovery obligations; an issue the Department of Justice’s own Office of the Inspector General has identified as concerning (*See* DOJ OIG Annex to the Report on the President’s Surveillance Program, July 10, 2009, at 35 (“We found that the Department made little effort to understand and comply with its discovery obligations ... We believe that the Department should consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA...”)) <https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf>). Rule 16(a)(1)(E)(i) requires the government to produce “item[s] material to preparing the defense”, we submit that this includes items material to making a suppression motion under Rule 12(b)(3)(C). *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993) (Under Rule 16(a)(1)(c), the predecessor to Rule 16(a)(1)(E)(i), evidence “is material if it could be used to counter the government’s case or to bolster a defense.”). Further, even if that were not the case, Rule 16 (a)(1)(B)(i) commands the government to produce as part of discovery “any relevant written or recorded statement by the defendant...within the government’s possession, custody, or control; and [that] the attorney for the government knows – or through due diligence could know - ... exists”. The information requested by the defense falls squarely within each of these categories.

Moreover, notions of justice, fundamental fairness and due process command that the defendants not be required to wait until the eve of trial or worse, until trial, to vindicate their rights. The statutes do not contemplate that to be the case, nor have the courts held that to be so. Indeed, in *United States v. Ishan Sharif Khawaja* 05 CR 830 (HB), the Honorable Harold Baer ordered the government, in the context of discovery motion, to respond to a virtually identical request – even in the face of a representation from the Assistant United States Attorney assigned to handle the matter that no statements of the defendant were recorded. In that case, the only asserted grounds for the request were that the defendant and his family were of Afghani descent, the defense believed that post-9/11 the family was investigated to determine whether they had links to terrorism, and the case agent in the transshipment case was a member of the joint terrorism task force. Notably, even before the issue was addressed by the Court, consistent with

LAW OFFICES OF

GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 10

CRM 36, the government submitted a request for the information to the Department of Justice, without objection. *See* Exhibit “C”.

Conclusion

As the Supreme Court so aptly stated in *United States v. United States District Court*, *supra*:

...Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. *Katz v. United States*, at 359-360 (DOUGLAS, J., concurring). But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

407 U.S. at 316-17. As government intelligence capabilities and activities expand beyond anything our founding fathers possibly could have imagined, the role of the judiciary as a check on unfettered executive power is ever more important.

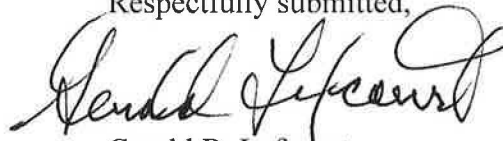
In the context of this case, with these facts, and in the face of the government’s responses, it is inconceivable that the government did not seek to intercept the defendants’ oral and written communications by means other than Title III warrants. The defendants are entitled to know the extent of the government’s non-Title III surveillance and interceptions and any evidence derived

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

Honorable J. Paul Oetken
United States District Judge
Southern District of New York
December 12, 2019
Page 11

therefrom, to challenge such conduct, and vindicate their constitutional rights and privacy interests.

Respectfully submitted,



Gerald B. Lefcourt

cc: All counsel (via ecf)